UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/824,595	04/02/2001	Randall Scott Springfield	RPS9 2000 0016	1231

47052 7590 12/09/2008
IBM RP-RPS
SAWYER LAW GROUP LLP
2465 E. Bayshore Road, Suite No. 406
PALO ALTO, CA 94303

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
12/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@sawyerlawgroup.com

Office Action Summary	**Application No.** 09/824,595	**Applicant(s)** SPRINGFIELD ET AL.	
	Examiner Thomas Gyorfi	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6-12 and 15-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6-12 and 15-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1, 2, 6-12, and 15-21 remain for examination. The correspondence filed 9/30/08 amended claims 1, 2, 6, & 10; and added claims 18-21.

Response to Arguments

2. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claim 1 is objected to because of the following informalities: the claim recites "storing a trusted boot source in a first register from a peripheral connector"; as written, the claim language appears to suggest that the first register is located within the peripheral connector, rather than the bridge as disclosed by the instant specification. For the sake of clarity, Examiner suggests that the phrase be rewritten as “storing a trusted boot source from a peripheral connector in a first register” to mitigate the ambiguity. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 2, 6-12, and 15-21 rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for “storing identification information for a trusted boot source

in a first register", does not reasonably provide enablement for storing the entire trusted boot source in said first register. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make the invention commensurate in scope with these claims. Independent claims 1 and 6 were specifically amended to now recite that the trusted boot source is stored in full in the first register, but the specification contradicts this arrangement, most clearly with Figure 2. The registers that are central to the invention inhabit the bridge component (120), whereas the boot sources exist either in Flash Boot source (140) or in an un-illustrated element that is directly connected to the peripheral connector (130) (specification, page 5, lines 13-16). Furthermore, all references as to the contents of said registers specifically refer to storing identities of the various boot sources in the invention, and not the boot sources themselves (e.g. page 6, lines 1-11). Dependent claims 2, 7-12, and 15-21 are rejected by virtue of their dependencies on claims 1 and 6, as appropriate. For purposes of examination, Examiner has assumed that the claimed registers store only the recited identification information, as is taught and supported by the instant specification.

6. Also, claims 2 and 10 are further rejected under 35 USC 112, 1st paragraph, as the claims were amended to now recite wherein the first register, rather than the trusted boot source, is a flash memory device. Again, the instant specification only stipulates that the memory devices where the boot sources are stored are flash memory devices, but says nothing about the particular memory technology used to implement the registers. And, as discussed *supra*, the specification does not support storing the trusted boot source in any of the registers; only identities thereof may be stored therein. For purposes of examination, Examiner has assumed

that the claims are referring to the boot sources being flash memory devices, again as supported by the specification.

Claim Rejections - 35 USC § 101

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claim 11 is rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claim 11 recites wherein the **first** register - which according to parent claim 6, contains the trusted boot source identity in a **write-once** register - has the identity of the actual boot source written to it **each time the computer system boots**. Clearly, the fact that the first register of the parent claim cannot by definition be re-written, coupled with the fact that the one and only write operation permitted upon it was used to store the *trusted* boot source and not the *actual* boot source as recited in claim 11, renders the claimed invention inoperable. Examiner respectfully suggests that this rejection may be overcome by amending the claim to recite wherein it is the *second* register that is operated in the recited fashion, as would be supported by the instant specification and also by common sense.

Claim Rejections - 35 USC § 103

9. Any invocations of Official Notice from the Office Action of 6/5/08 that were not traversed by the Applicant in the amendment of 9/30/08 are now taken as Applicant admissions of prior art, as provided by MPEP 2144.03(c).

10. Claims 1, 2, 6-8, 10-12, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock et al. (U.S. Patent 6,678,833) in view of Jablon et al. (U.S. Patent 5,421,006) in view of Poisner (U.S. Patent 6,920,553).

Regarding claim 1:

Grawrock discloses a method for verifying a boot source having a processor comprising: storing [an identity of] a trusted boot source in a first register, the first register comprising a write-once register (col. 3, lines 63-67); determining identification information of an actual boot source used by the processor each time the computer system boots including examining a location of a predetermined number of instructions initially executed during boot up (col. 3, lines 40-60; col. 4, lines 20-35) in order to prevent an unscrupulous boot source from being loaded (col. 4, lines 35-40).

It is observed that the Grawrock disclosure is primarily focused on how one creates the identifiers by which an evaluation of whether the boot source being used is trusted, while disclosing minimal information as to exactly how the comparison is made. Thus, it is unclear whether Grawrock compares the various disclosed registers against each other. However, Jablon discloses an analogous method for verifying a trusted boot source (e.g. col. 2, lines 25-35) by comparing an identity of an actual boot source (the boot source being explicitly disclosed as being a predetermined number of instructions initially executed at boot-up: col. 11, lines 55-67) against a copy of the identity of the trusted boot source stored in write-protected memory (see the “bootCode” and “confiCode”: col. 12, line 5 – col. 13, line 15), again so as to prevent an unscrupulous boot source from being loaded (col. 7, lines 60-65)). The claim is thus obvious because the technique of comparing the identity of an actual boot source against the identity of a trusted boot source had long since been recognized as being within the ordinary capabilities of one skilled in the art.

Although Grawrock discloses wherein the boot source(s) are connected to a link, and the hardware implementing the invention is capable of supporting such peripheral connecting links such as PCI, USB, and the like (col. 3, lines 5-15). Nevertheless, the technique of loading a boot source through a peripheral connector was well known in the prior art; one such example is disclosed by Poisner (via USB at col. 2, lines 10-25; noting that prior art techniques involving booting via a PCI card were also well known: col. 1, lines 40-60). Poisner even discloses wherein one should perform some authentication technique to ensure that one may trust the boot source being loaded in such a fashion (col. 2, lines 40-50). The claim is thus obvious because the technique of booting from a boot source via a peripheral connector had also long since been recognized as being within the ordinary capabilities of one skilled in the art; the technique also has utility in that it would still allow one to boot one's computer if the on-board BIOS were ever corrupted or missing (col. 1, lines 40-45).

Regarding claim 6:

Grawrock discloses a system for verifying a boot source in a computer system having a processor coupled with a boot source, comprising: a first register, comprising a write-once register, the first register for storing the identity of a trusted boot (col. 3, lines 63-67); a bridge, coupled in communication with the first register, the bridge to determine identification information of an actual boot source used by the processor each time the computer system boots including examining a location of a predetermined number of instructions initially executed boot-up (col. 3, lines 40-60; col. 4, lines 20-35; Figures 2 & 3); and a second register, coupled in communication with the bridge, the second register to store an idenfication information of the actual boot source (Ibid).

It is observed that the Grawrock disclosure is primarily focused on how one creates the identifiers by which an evaluation of whether the boot source being used is trusted, while disclosing minimal information as to exactly how the comparison is made. Thus, it is unclear whether Grawrock compares the various disclosed registers against each other. However, Jablon discloses an analogous method for verifying a trusted boot source (e.g. col. 2, lines 25-35) by comparing an identity of an actual boot source (the boot source being explicitly disclosed as being a predetermined number of instructions initially executed at boot-up: col. 11, lines 55-67) against a copy of the identity of the trusted boot source stored in write-protected memory (see the “bootCode” and “confiCode”: col. 12, line 5 – col. 13, line 15), again so as to prevent an unscrupulous boot source from being loaded (col. 7, lines 60-65)). The claim is thus obvious because the technique of comparing the identity of an actual boot source against the identity of a trusted boot source had long since been recognized as being within the ordinary capabilities of one skilled in the art.

Although Grawrock discloses wherein the boot source(s) are connected to a link, and the hardware implementing the invention is capable of supporting such peripheral connecting links such as PCI, USB, and the like (col. 3, lines 5-15). Nevertheless, the technique of loading a boot source through a peripheral connector was well known in the prior art; one such example is disclosed by Poisner (via USB at col. 2, lines 10-25; noting that prior art techniques involving booting via a PCI card were also well known: col. 1, lines 40-60). Poisner even discloses wherein one should perform some authentication technique to ensure that one may trust the boot source being loaded in such a fashion (col. 2, lines 40-50). The claim is thus obvious because the technique of booting from a boot source via a peripheral connector had also long since been recognized as being within the ordinary capabilities of one skilled in the art; the technique also has utility in that it would still allow one to boot one's computer if the on-board BIOS were ever corrupted or missing (col. 1, lines 40-45).

Regarding claims 2 and 10:

It is now accepted as Applicant admitted prior art that the boot sources used in the disclosed prior art inventions would be FLASH boot sources.

Regarding claim 7:

Grawrock further teaches wherein the computer system includes a bridge couples the processor with the actual boot source and wherein the first register and the second register are located within the bridge (col. 3, lines 7-24; Figures 2 and 3).

Referring to claim 8:

Grawrock further discloses wherein the bridge is a south bridge (the input/output control hub: element 140 of Figure 1; col. 3, lines 18-24).

Regarding claim 11:

Grawrock further discloses wherein the identity of the actual boot source is written to the appropriate register each time the computer system boots (col. 3, 62-63).

Regarding claim 12:

Grawrock and Jablon further disclose wherein the processor is capable of checking the boot source stored in the first register to ensure that the boot source is the known boot source (Grawrock: col. 4, lines 35-40; Jablon: col. 12, lines 25-50).

Regarding claims 16 and 17:

Jablon further discloses shutting down the computer system responsive to the actual boot source not matching the trusted boot source (col. 13, lines 10-15).

Regarding claims 18 and 20:

Poisner further discloses wherein the peripheral connector comprises a PCI connector (col. 1, lines 40-60).

Regarding claims 19 and 21:

Poisner further discloses wherein the actual boot source is coupled to the peripheral connector (col. 2, lines 50-60).

11. Claims 9 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock in view of Jablon in view of Poisner as applied to claims 1 & 6 above, and further in view of Davis et al. (U.S. Patent 6,401,208).

Regarding claims 9 and 15:

Neither Grawrock nor Jablon nor Poisner explicitly disclose wherein the trusted boot source identifier is written to the register *during the manufacture of the computer system.* However, Davis discloses an analogous method of authenticating a trusted BIOS boot source, wherein the information necessary to provide the authentication of the trusted BIOS is written into write-once memory at the time of the computer's manufacture (col. 4, lines 40-60; col. 5, lines 10-15). The claims are thus obvious because a person of ordinary skill in the art would have a good reason to pursue the known options within one's technical grasp. If writing the authentication information employed by Grawrock and/or Jablon into the write-once register at the time of the computer's manufacture would lead to success, it would likely be the product not of innovation but of ordinary skill and common sense. See *KSR v. Teleflex*, 550 U.S. at ___, 82 USPQ2d at 1397.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure, each of which further support the conclusion that connecting a boot source to a peripheral connector was an obvious technique:

- U.S. Patent 6,425,079 to Mahmoud (e.g. Figures 1-4)
- U.S. Patent 6,185,678 to Arbuagh et al. (e.g. Figure 1c)

- U.S. Patent 6,170,049 to So (e.g. Figure 29)
- U.S. Patent 5,802,393 to Begun et al. (e.g. Figure 1)

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
11/24/08
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435